Innovative Instructions and Software Model for Isolated Execution

Frank McKeen (frank.mckeen@intel.com),
Ilya Alexandrovich (ilya.alexandrovich@intel.com),
Alex Berenzon (alex.berenzon@intel.com),
Carlos V Rozas (carlos.v.rozas@intel.com),
Hisham Shafi (hisham.shafi@intel.com),
Vedvyas Shanbhogue (vedvyas.shanbhogue@intel.com),
Uday R Savagaonkar (uday.r.savagaonkar@intel.com)

Abstract:
For years the PC community has struggled to provide secure solutions on open platforms. Intel has developed innovative new technology to enable SW developers to develop and deploy secure applications on open platforms. The technology enables applications to execute with confidentiality and integrity in the native OS environment. It does this by providing ISA extensions for generating hardware enforceable containers at a granularity determined by the developer. These containers while opaque to the operating system are managed by the OS. This paper analyzes the threats and attacks to applications. It then describes the ISA extension for generating a HW based container. Finally it describes the programming model of this container.

HASP '13, Jun 23-24 2013, Tel-Aviv, Israel
ACM 978-1-4503-2118-1/13/06.